CLAIMS

What is claimed is:

1. A method comprising:

generating a formal license for content that includes:

a decryption key for decrypting the content; and

access rules for accessing the content; and

configuring a plurality of license authorities to provide a plurality of partial licenses, wherein:

each said license authority provides a respective said partial license; and

the plurality of partial licenses are combinable to form the formal license.

2. A method as described in claim 1, wherein the plurality of partial licenses are provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

3. A method as described in claim 1, wherein the configuring includes:

generating a pre-license from the formal license by encrypting the formal license;

dividing an encryption key into a plurality of partial secret shares, wherein the encryption key is for decrypting the pre-license; and

transmitting the pre-license and a respective said partial secret share to each said

license authority such that each said license authority is configured to generate the respective said partial license from the respective said partial secret share and the pre-license.

4. A method as described in claim 3, wherein each said license authority verifies the pre-license and the respective said partial secret share by utilizing a verifiable secret sharing (VSS) scheme.

5. A method as described in claim 1, wherein the configuring includes:

generating a pre-license from the formal license by encrypting the formal license utilizing an asymmetric encryption algorithm having a public key and a private key, wherein the formal license, the pre-license and the public key are denoted, respectively, as "*license*", "*prel*" and "*PK*" as follows:

$$prel = (license)^{pk};$$

dividing the private key *SK* into *m* partial secret shares according to a (*k, m*) threshold secret sharing scheme by:

generating a sharing polynomial *f(x)* over any finite field *Z*, where a_o = *SK*, the sharing polynomial being represented as follows:

$$f(x) = a_o + a_1 x + \ldots + a_{k-1} x^{k-1}; \text{ and}$$

calculating each said partial secret share, denoted as S_i, for a respective said license authority, denoted by id_i, in which $i = 1, \ldots, m$, as follows:

$$S_i = f(id_i); \text{ and}$$

transmitting the pre-license and a respective said partial secret share to a

respective said license authority, wherein each said license authority is configured to generate the respective said partial license from the respective said partial secret share and the pre-license.

6. A method as described in claim 5, wherein each said license authority verifies the pre-license and the respective said partial secret share by utilizing a verifiable secret sharing (VSS) scheme in which k public witnesses of the sharing polynomial's $f(x)$ coefficients (denoted as $\{g^{a_0},\cdots;g^{a_{k-1}}\}$, where $g \in Z$) are communicated to each said license authority id_i to verify validity of a respective said partial secret share S_i by determining if the following equation holds:

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}}$$

7. A method as described in claim 1, further comprising packaging the content to include one or more network addresses that are suitable for locating each said license authority.

8. A method as described in claim 1, wherein each said license authority is communicatively coupled to a peer-to-peer network.

9. A method as described in claim 1, wherein the plurality of license authorities are configured based on a consideration such that at least one said license authority provides two or more said partial licenses, wherein the consideration is selected

from the group consisting of:

security of the at least one said license authority against unauthorized access;

load sharing of the plurality of license authorities;

availability of each said license authority;

network availability of each said license authority;

hardware resources of each said license authority;

software resources of each said license authority; and

any combination thereof.

10. A method as described in claim 1, wherein the configuring includes transmitting the plurality of partial licenses to the plurality of license authorities such that each said license authority stores the respective said partial license.

11. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 1.

12. A computer-readable medium comprising computer executable instructions that, when executed by a computer, direct the computer to:

configure a plurality of license authorities to provide a plurality of partial licenses, wherein:

each said license authority provides a respective said partial license;

each said license authority has a network address;

the plurality of partial license are combinable to form a formal license; and

the formal license provides access to content; and

package the content to include one or more network addresses that are suitable for locating each said license authority.

13. A computer-readable medium as described in claim 12, wherein the one or more network addresses include one or more proxy addresses for locating a network address of each said license authority.

14. A computer-readable medium as described in claim 12, wherein the one or more network addresses include a network address of each said license authority.

15. A computer-readable medium as described in claim 12, wherein the plurality of license authorities are configured to provide the plurality of partial licenses according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

16. A computer-readable medium as described in claim 12, wherein the computer executable instructions when executed by the computer direct the computer to configure a plurality of license authorities by:

generating a pre-license from the formal license by encrypting the formal license;

dividing an encryption key into a plurality of partial secret shares, wherein the encryption key is for decrypting the pre-license; and

transmitting the pre-license and a respective said partial secret share to each said license authority such that each said license authority is configured to generate the respective said partial license from the respective said partial secret share and the pre-license.

17. A computer-readable medium as described in claim 16, wherein each said license authority verifies the pre-license and the respective said partial secret share by utilizing a verifiable secret sharing (VSS) scheme.

18. A computer-readable medium as described in claim 12, wherein the computer executable instructions, when executed by the computer, direct the computer to configure the plurality of license authorities by transmitting the plurality of partial licenses to the plurality of license authorities such that each said license authority stores the respective said partial license.

19. A computer-readable medium comprising computer executable instructions that, when executed by a computer, direct the computer to:

encrypt content;

generate a formal license for the encrypted content that includes access rules and a decryption key for decrypting the encrypted content;

encrypt the formal license to generate a pre-license;

divide an encryption key suitable for decrypting the pre-license into a plurality of partial secret shares;

upload the pre-license and the plurality of partial secret shares to a plurality of license authorities such that each said license authority receives a respective said partial secret share and the pre-license;

package the encrypted content to include one or more network addresses that are suitable for locating each said license authority; and

distribute the packaged content.

20. A computer-readable medium as described in claim 19, wherein the plurality of license authorities are configured to provide the plurality of partial licenses according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

21. A computer-readable medium as described in claim 19, wherein each said license authority verifies the pre-license and the respective said partial secret share by utilizing a verifiable secret sharing (VSS) scheme.

22. A method comprising:

obtaining a plurality of partial licenses over a network from a plurality of license

authorities, wherein each said partial license is provided, respectively, by a different said license authority; and

forming a formal license from the plurality of partial licenses, wherein the formal license includes access rules and a decryption key for accessing content.

23. A method as described in claim 22, wherein the obtaining includes:

examining the content to find a plurality of network addresses of a plurality of license authorities;

requesting the plurality of partial licenses from the plurality of license authorities; and

receiving one or more communications having one or more said partial licenses that are provided by each said license authority.

24. A method as described in claim 22, wherein the forming includes combining the plurality of partial licenses to form the formal license.

25. A method as described in claim 22, wherein the plurality of partial licenses are provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

26. A method as described in claim 25, further comprising determining if k correct partial licenses have been received.

27. A method as described in claim 22, wherein:

the plurality of partial licenses are obtained from the plurality of license authorities over a finite field Z by:

calculating the partial license $prel_i$ by each said license authority id_i from a partial secret share S_i and a pre-license $prel$ according to the following equation:

$$prel_i = (prel)^{S_i};$$

generating a random number u to calculate $A_1 = g^u$, $A_2 = prel^u$, $r = u - c * S_i$, and

$$c = hash\,(g^{S_i}, prel_i, A_1, A_2)\,;\text{ and}$$

communicating the partial license $prel_i$, A_1, A_2, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by validating each said partial license $prel_i$ by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}}$$

from public witnesses of a sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \cdots; g^{a_{k-1}}\}$, that was utilized to generate the partial secret share S_i, where $g \in Z$,

applying $c = hash(g^{S_i}, prel_i, A_1, A_2)$ to calculate c; and

checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license $prel_i$, and if so, each said partial license $prel_i$ is valid; and

combining the plurality of partial licenses to form the formal license, denoted as *license*, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$
$$= (prel)^{SK} = ((license)^{PK})^{SK},$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}$.

28. One or more computer-readable media comprising computer-executable instructions that, when executed, perform the method as recited in claim 22.

29. A computer-readable medium comprising computer executable instructions that, when executed by a computer, direct the computer to:

examine packaged content to find a plurality of network addresses of a plurality of license authorities;

request a plurality of partial licenses from the plurality of license authorities;

receive the plurality of partial licenses from the plurality of license authorities, wherein each said license authority provides at least one said partial license;

combine the plurality of partial licenses to form a formal license, wherein the

formal license includes access rules and a decryption key for decrypting the packaged content; and

output the content by decrypting the packaged content utilizing the encryption key and checking the access rules of the formal license.

30. A computer-readable medium as described in claim 29, wherein the plurality of partial licenses are provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

31. A method comprising:

configuring a plurality of license authorities in a first arrangement to provide a plurality of partial licenses, wherein:

each said license authority provides at least one said partial license; and

the plurality of partial licenses are combinable to form a formal license that includes access rules and a decryption key for content; and

updating the first arrangement to form a second arrangement such that:

each said license authority in the second arrangement provides at least one of a plurality of updated partial licenses that are combinable to form the formal license; and

the partial licenses provided in the first arrangement are not combinable with the updated partial licenses to form the formal license.

32. A method as described in claim 31, wherein the updating is performed periodically.

33. A method as described in claim 31, wherein the updating is performed over a finite field *Z* by:

generating a random *(k, m)* sharing by each license authority *i* using a random update polynomial $f_{i,\,update}(x)$, wherein:

$$f_{i,update}(x) = b_{i,1}x + \ldots + b_{i,k-1}x^{k-1}; \text{ and}$$

distributing a subshare S_{ij} by each said license authority *i* such that each said license authority *i* has a respective said subshare S_{ij} from another said license authority wherein:

the subshare $S_{i,j} = f_{i,update}(j)$, $j = 1, \cdots, m$ is calculated by each said license authority *i*;

the subshare S_{ij} is added to the original share S_i of each said license authority to form a new updated share

$$S_i' = S_i + \sum_{j=1}^{m} S_{j,i}\ ; \text{ and}$$

a new secret sharing polynomial $f_{new}(x)$ is formed which is a summation of an original polynomial $f(x)$ utilized to generate the plurality of partial licenses in

the first arrange and each of the randomly generated polynomials $f_{i,update}(x)$.

34. A content publisher comprising:

a processor; and

memory configured to maintain:

a formal license that includes access rules and a decryption key for content; and

a license module that is executable on the processor to form one or more transmissions that include data for configuring a plurality of license authorities such that:

each said license authority provides one of a plurality of partial licenses; and

the plurality of partial licenses are combinable to form the formal license.

35. A content publisher as described in claim 34, wherein the plurality of license authorities are configured to provide the plurality of partial licenses according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

36. A content publisher as described in claim 34, wherein:

the configuring includes:

generating a pre-license from the formal license by encrypting the formal license; and

dividing an encryption key into a plurality of partial secret shares, wherein the encryption key is for decrypting the pre-license; and

the one or more transmissions include the pre-license and the plurality of partial secret shares such that each said license authority is configured to generate a respective said partial license from a respective said partial secret share and the pre-license.

37. A content publisher as described in claim 34, wherein the configuring includes transmitting the plurality of partial licenses to the plurality of license authorities such that each said license authority stores the respective said partial license.

38. A digital rights management system comprising a peer-to-peer network having a plurality of nodes, wherein:

one said node includes a license module that is executable to form one or more transmissions, wherein each said transmission includes a pre-license and a partial secret share of an encryption key utilized to encrypt the pre-license;

at least two said nodes are each configured to generate a respective one of a plurality of partial licenses from a respective said partial secret share and the pre-license that is received from a respective said transmission; and

a number k of the partial licenses are combinable to form a formal license that

includes an encryption key and access rules for accessing content.

39. A digital rights management system as described in claim 38, wherein one or more said nodes provide the content.

40. A digital rights management system as described in claim 38, wherein knowledge of any $k - 1$ or fewer of the partial licenses may not be utilized to form information included in the formal license.

41. A digital rights management system comprising a peer-to-peer network having a plurality of nodes, wherein:

at least two said nodes are each configured to provide at least one of a plurality of partial licenses; and

one said node includes:

a digital rights management module for forming a formal license from the plurality of partial licenses, wherein the formal license includes access rules and a decryption key for decrypting encrypted content; and

a content player for outputting content that is accessed utilizing the formal license.

42. A digital rights management system as described in claim 41, wherein the plurality of partial licenses are provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

43. A client device comprising:

a processor; and

memory configured to maintain:

packaged content that includes one or more network addresses that are suitable for locating a plurality of license authorities, wherein each said license authority stores one or more partial licenses;

a content player that is executable on the processor to output content; and

a digital rights management module that is executable on the processor to:

obtain the partial licenses from the plurality of license authorities utilizing the one or more network addresses; and

form a formal license from the obtained partial licenses, wherein the formal license provides access to the packaged content for output by the content player.

44. A client device as described in claim 43, wherein the digital rights management module that is executable on the processor to obtain the partial licenses by:

examining the packaged content to find the one or more network addresses of the plurality of license authorities;

requesting one or more said partial licenses from each said license authority; and

receiving one or more communications having the one or more partial licenses that are provided by each said license authority.

45. A client device as described in claim 43, wherein the plurality of partial licenses are provided according to a (k, m) threshold secret sharing scheme in which:

a number k said partial licenses are combinable to form the formal license; and

knowledge of any $k - 1$ or fewer said partial licenses may not be utilized to form information included in the formal license.

46. A client device as described in claim 43, wherein the one or more network addresses include a proxy address for locating a network address of each said license authority.

47. A client device as described in claim 43, wherein the one or more network addresses include a network address of each said license authority.

48. A client device as described in claim 43, wherein the digital rights management module that is executable on the processor to:

obtain the partial licenses from the plurality of license authorities, wherein each said license authority provide a respective said partial license over a finite field Z by:

calculating the partial license $prel_i$ by each said license authority id_i from a

partial secret share S_i and a pre-license *prel* according to the following equation:

$$prel_i = (prel)^{S_i};$$

generating a random number u to calculate $A_1 = g^u$, $A_2 = prel^u$, $r = u - c * S_i$, and

$$c = hash\,(g^{S_i}, prel_i, A_1, A_2)\,;\text{ and}$$

communicating the partial license $prel_i$, A_1, A_2, and r by each said license authority; and

the formal license is formed from the plurality of partial licenses by:

determining if k correct partial licenses have been received by validating each said partial license $prel_i$ by:

calculating

$$g^{S_i} = g^{a_0} \cdot (g^{a_1})^{id_i} \cdot \ldots \cdot (g^{a_{k-1}})^{id_i^{k-1}}$$

from public witnesses of a sharing polynomial's coefficients, which are denoted as $\{g^{a_0}, \cdots; g^{a_{k-1}}\}$, that was utilized to generate the partial secret share S_i, where $g \in Z$,

applying $c = hash\,(g^{S_i}, prel_i, A_1, A_2)$ to calculate c; and

checking if $g^r \cdot (g^{S_i})^c = A_1$ and $prel^r \cdot (prel_i)^c = A_2$ hold for each said partial license $prel_i$, and if so, each said partial license $prel_i$ is valid; and

combining the plurality of partial licenses to form the formal license, denoted as *license*, when k valid said partial licenses are obtained, in which:

$$license = \prod_i (prel_i)^{l_{id_i}(0)} = (prel)^{\sum_i S_i \cdot l_{id_i}(0)}$$

$$= (prel)^{SK} = ((license)^{PK})^{SK},$$

where $l_{id_i}(x) = \prod_{j=1, j \neq i}^{k} \frac{x - id_j}{id_i - id_j}$.